Integration of OS Patches in COE 4.2

DII COE Developer's Conference

23 May 2000

Erik King

Agenda

- **COE 4.2 Security Lockdown**
- **Unix & Windows NT Implementations**
- **Lockdown Impact / Issues**
- **COE 4.2 OS Patch Integration Solution**
- **OS Patch Integration Process for DII COE**
- **Current OS Patch Segments / Status**
- **COE Developer / Integrator Guidance & Resources**

COE 4.2 Security Lockdown

- **COE 4.2 kernel installation enforces security lockdown**
- **Security "lockdown" events include:**
  - **Changes to directory and file permissions**
  - **Changes to directory and file ownership & group assignment**
  - **Changes to the system umask setting (UNIX)**
  - **Modification of system configuration files**
    - **Example: disabling ftp, telnet via inetd.conf**
  - **Requiring installation of specific Service Packs (NT)**
  - **Changes to registry settings (NT)**

COE 4.2 Security Lockdown

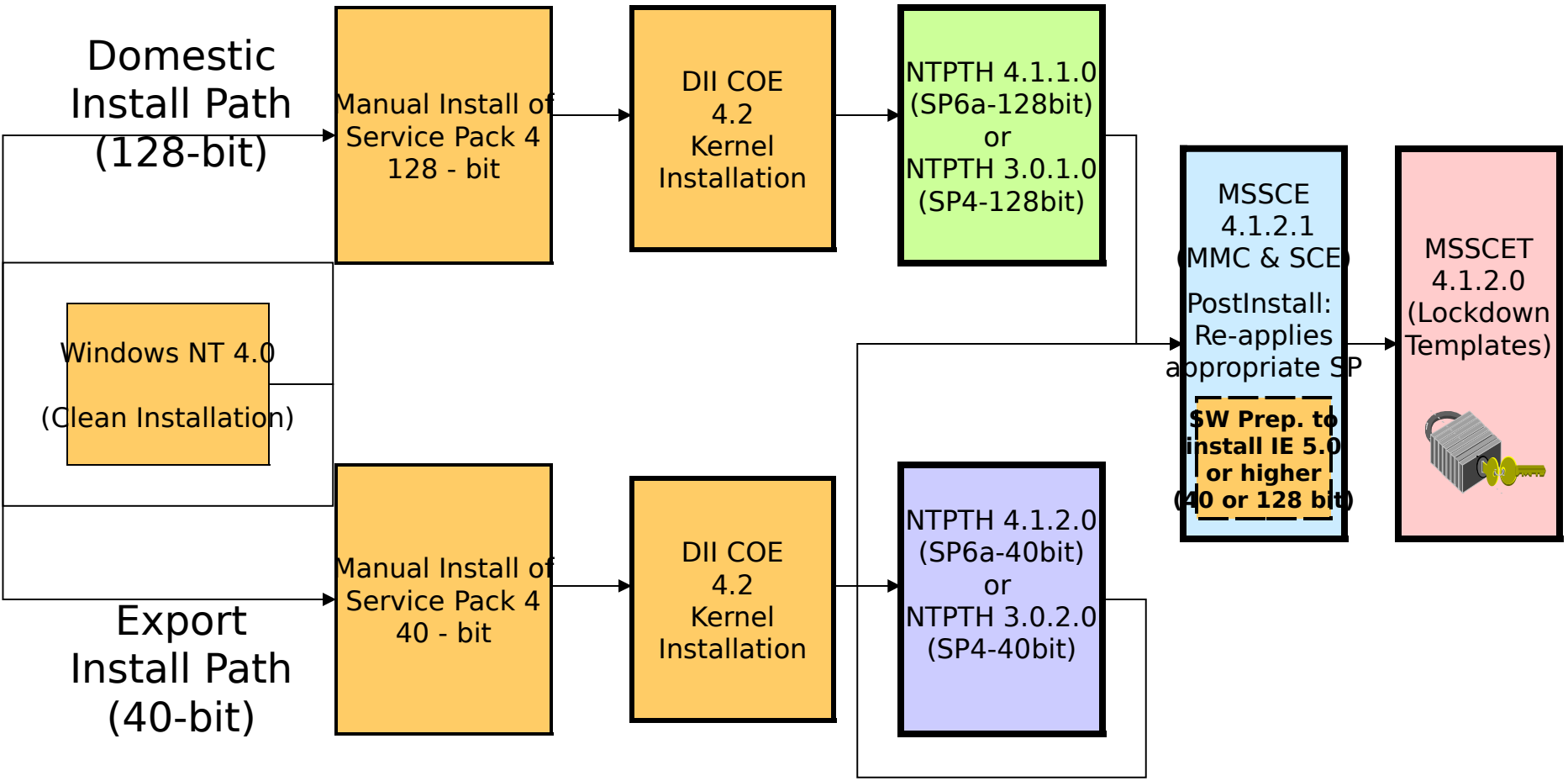
- **Security "lockdown" changes focus on:**
  - **File/Directory attribute changes**
  - **Configuration edits to ASCII-based files**
  - **File additions**

- **As of COE 4.1.2.0, changes do not include:**
  - **File/Directory replacements**
  - **Binary recompilations**

COE 4.2 Security Lockdown

- **How security lockdown is implemented:**
  - **Unix:**
    - **Implemented as part of the DII COE 4.2 Kernel Installation Routine**
  - **Windows NT:**
    - **Implemented as part of the DII COE 4.2 Kernel Installation Routine, and**
    - **Via security templates installed via the Microsoft Security Configuration Editor**
      - Segments: MSSCE, MSSCET

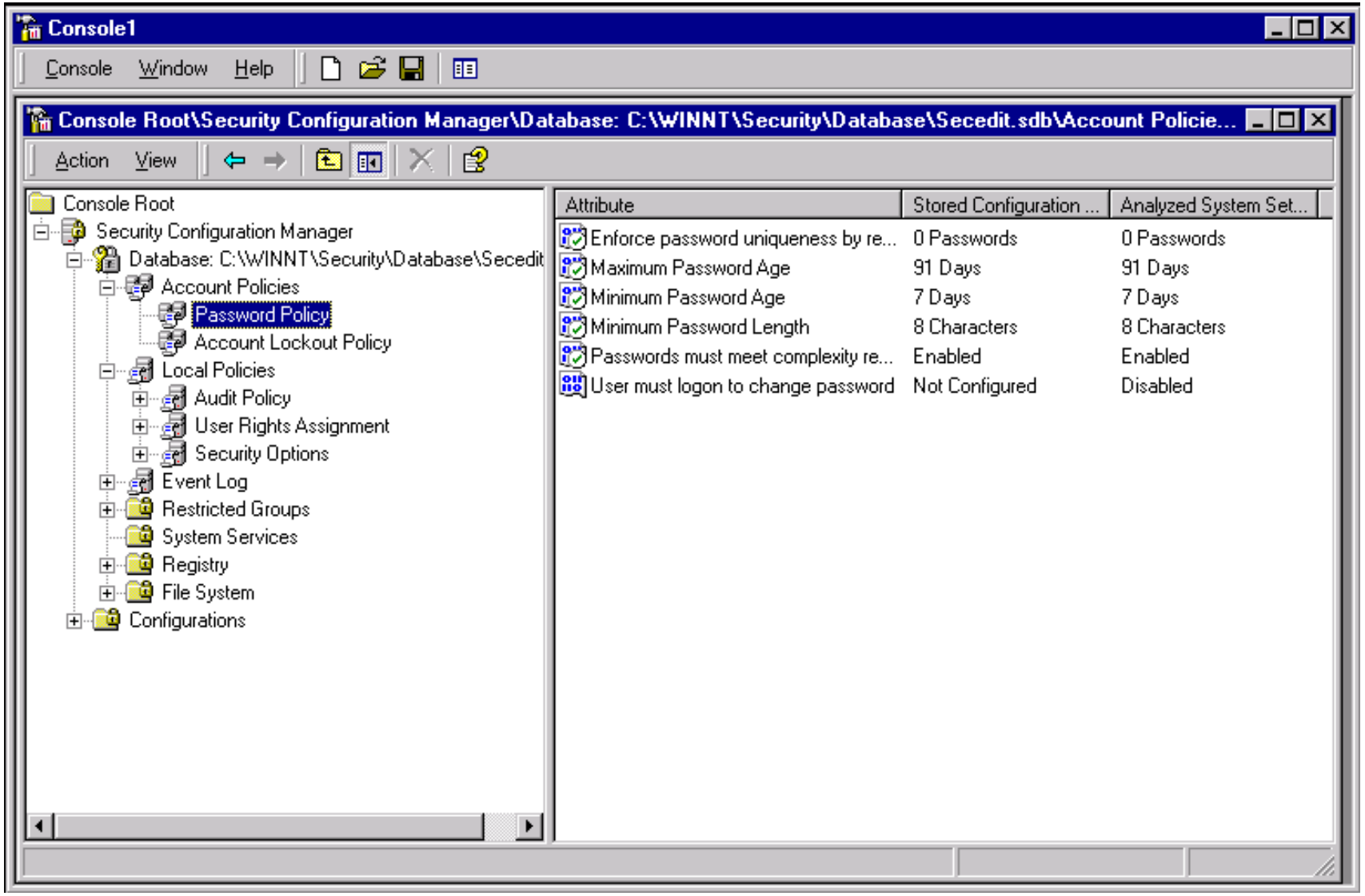
COE 4.2 - Windows NT Installation Sequence



COE 4.2 Security Lockdown

- **2 segments support NT lockdown:**
  - **MSSCE:**
    - **Contains the following COTS products:**
      - *MS Management Console (MMC)*
      - *MS Security Configuration Editor (SCE)*
    - **Provides the interface for NT security configuration**
    - **Requires IE 5.0 (or higher) to be loaded prior to installation**
  - **MSSCET:**
    - **Contains lockdown templates for three NT installation types:**
      - NT Workstation (WKS)
      - Standalone Server (SAS)
      - Primary / Backup Domain Controller (PDC/BDC)
    - **Templates can be customized for specific site implementation**

COE 4.2 Security Lockdown



COE 4.2 Security Lockdown

"Who wants to be a COE millionaire" $1M

Question:

- **How many Operating System files does the DII COE 4.2 kernel (and associated template segments) "modify" or otherwise "alter" at install time? (all platforms)**

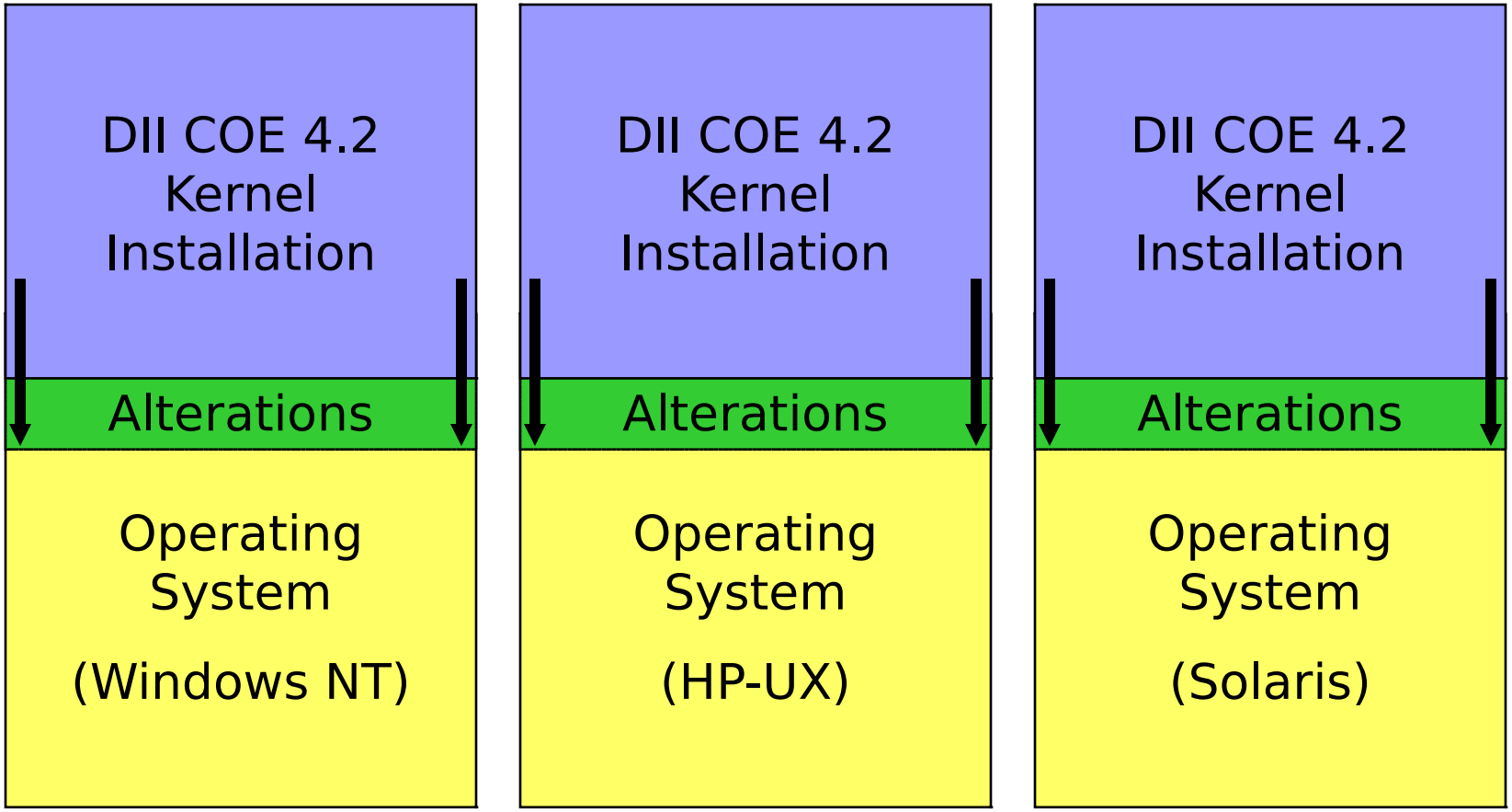
A: 0 - 50

B: 51 - 499 ***Correct Answer !!***

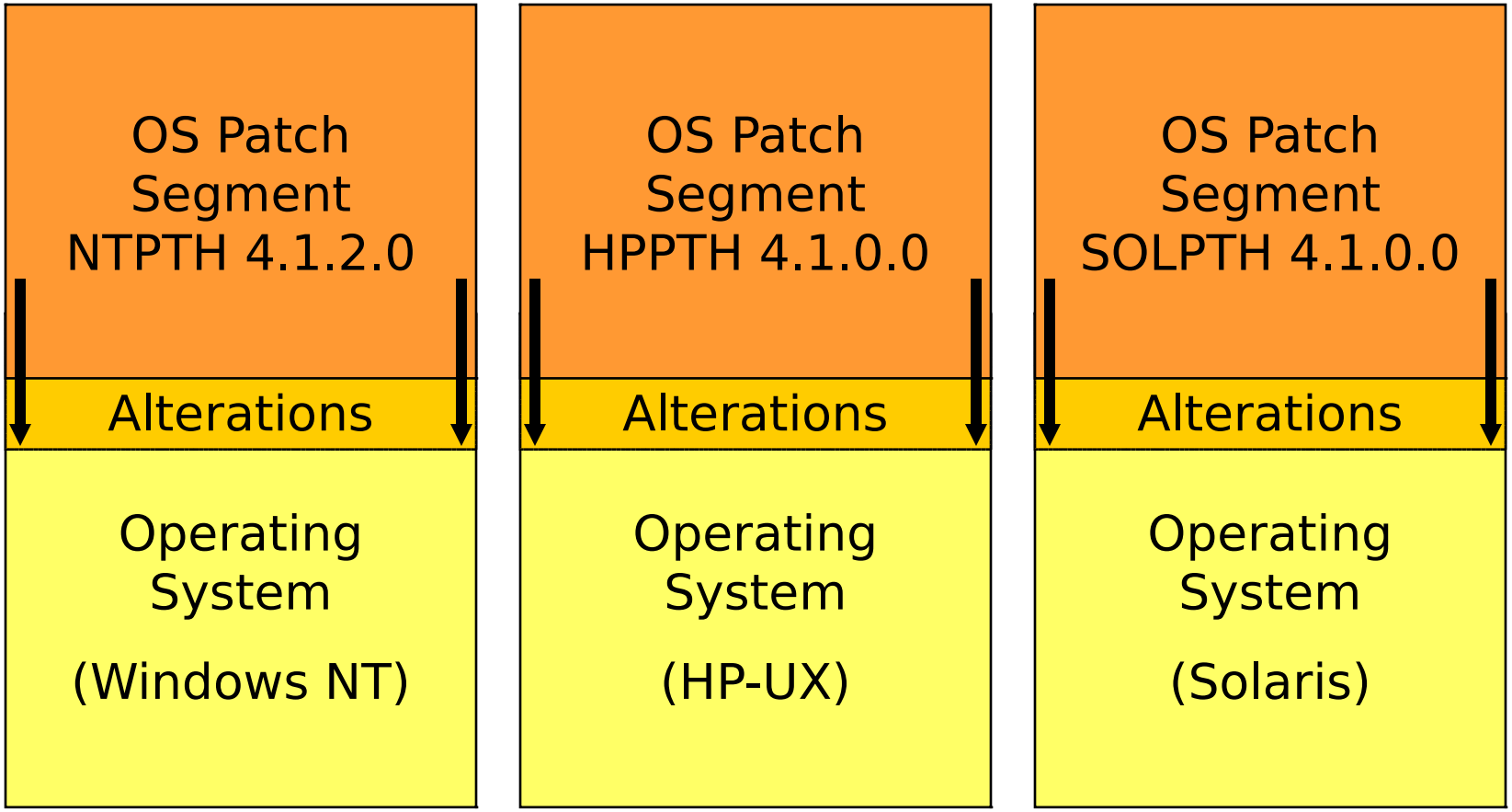
C: 500 - 999

D: Over 1,000

COE 4.2 Security Lockdown

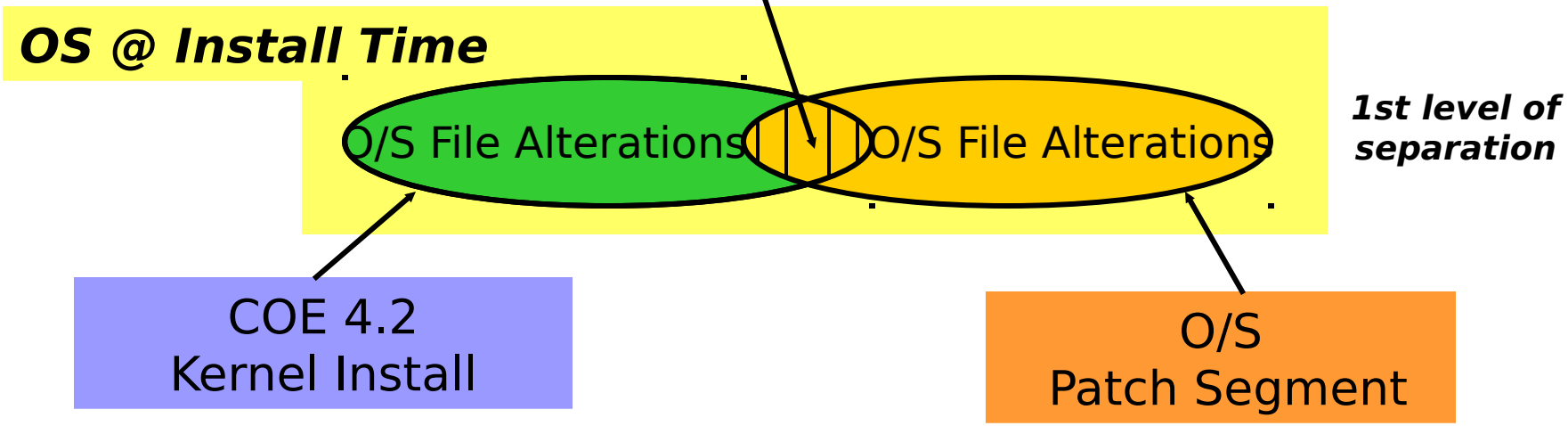


COE 4.2 Security Lockdown

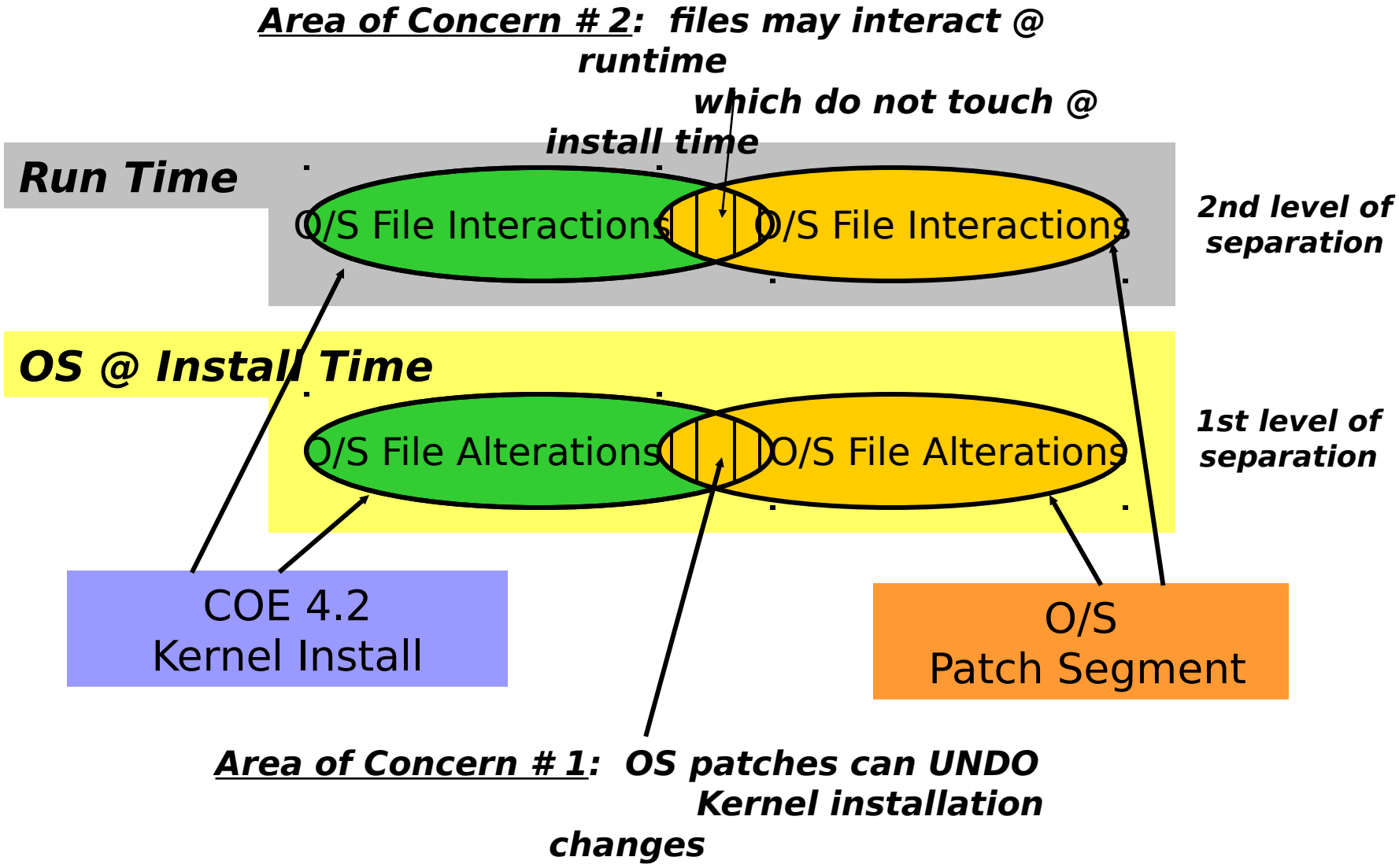


OS patch / kernel install issue

Area of Concern # 1: ***OS patches can UNDO Kernel installation changes***



OS patch / kernel install issue

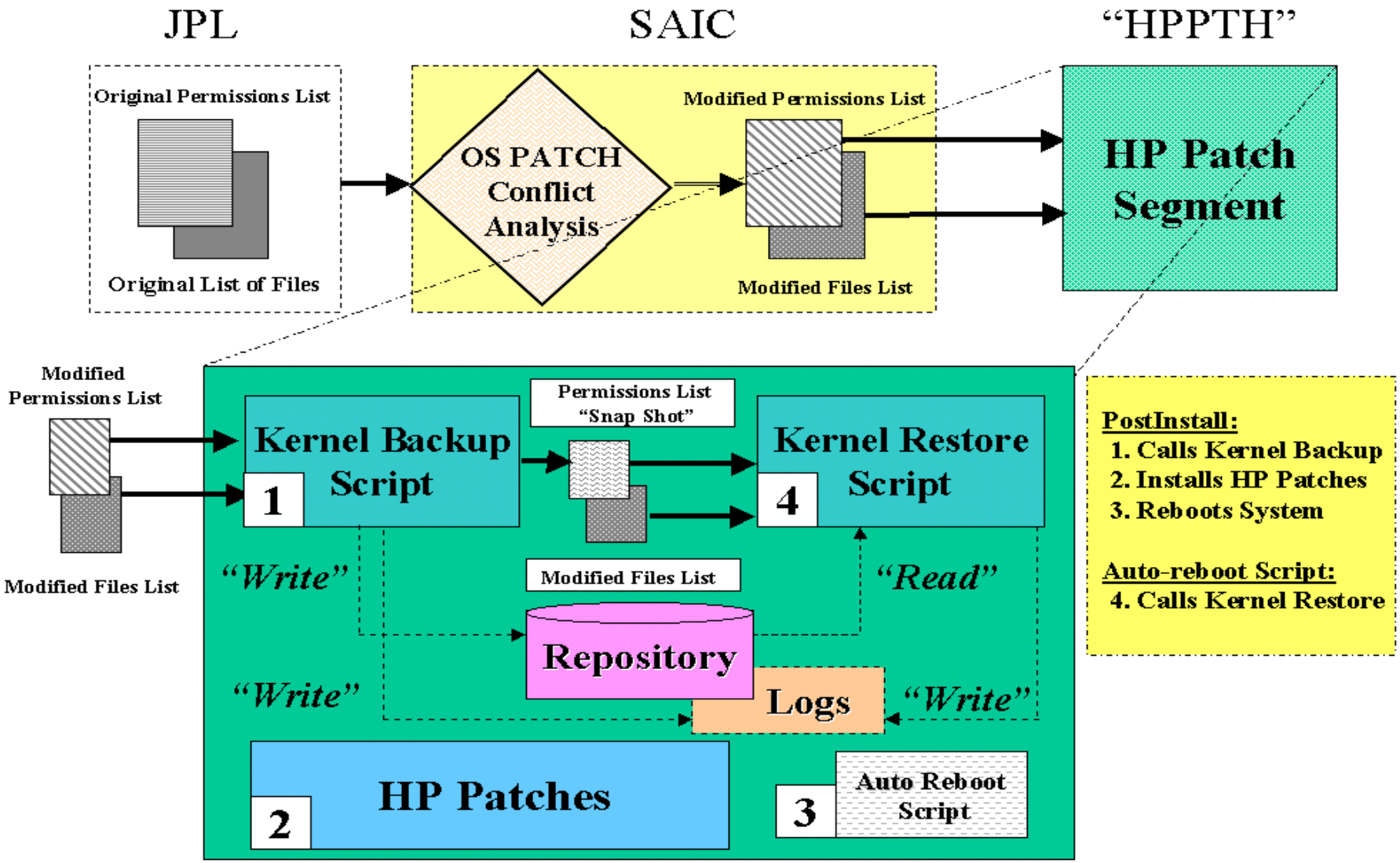


OS patch / kernel install issue

- ***Area of Concern # 1*: OS patches can UNDO kernel installation changes**
  - **Unix:**
    - **OS Patch segments (HPPTH 4.1.0.0 & SOLPTH 4.1.0.0) provide backup & restore capability of kernel security enhancements**
  - **Windows NT:**
    - **No impact noted for SP4 or SP6a**
    - **Integration team will implement backup & restore capability as need arises.**

- ***Area of Concern # 2*: files may interact @ runtime which do not touch @ install time**
  - **Resource intensive - identify & correct as needed**

OS Patch Integration Solution - UNIX



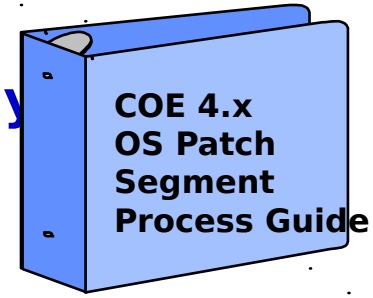
OS Patch Integration Solution

The bottom line:

- **Operating System patches require analysis and forethought prior to implementation in a COE environment**
- **Site integrators need to be aware of the issues and develop a methodology for implementing OS patches outside the COE scheduled process**

COE OS Patch Process

- ***COE OS patch releases adhere to a schedule driven methodology:***
  - **Step 1: Patch Acquisition & Prep. For analy**
  - **Step 2: Research & Analysis**
  - **Step 3: Development Announcement**
  - **Step 4: Begin Development**
  - **Step 5: Receipt of new requests / subsequent analysis**
  - **Step 6: Distribute “final” patch list**
  - **Step 7: Update / test / finalize OS patch segments**
  - **Step 8: CFI Delivery & subsequent testing & release**
- ***OS patch segments are released every 4 months***
- ***Currently working on 2nd set for Year 2000***



Current COE 4.2 OS Patch Segments

- **Current COE O/S Patch & Related Segment table:**

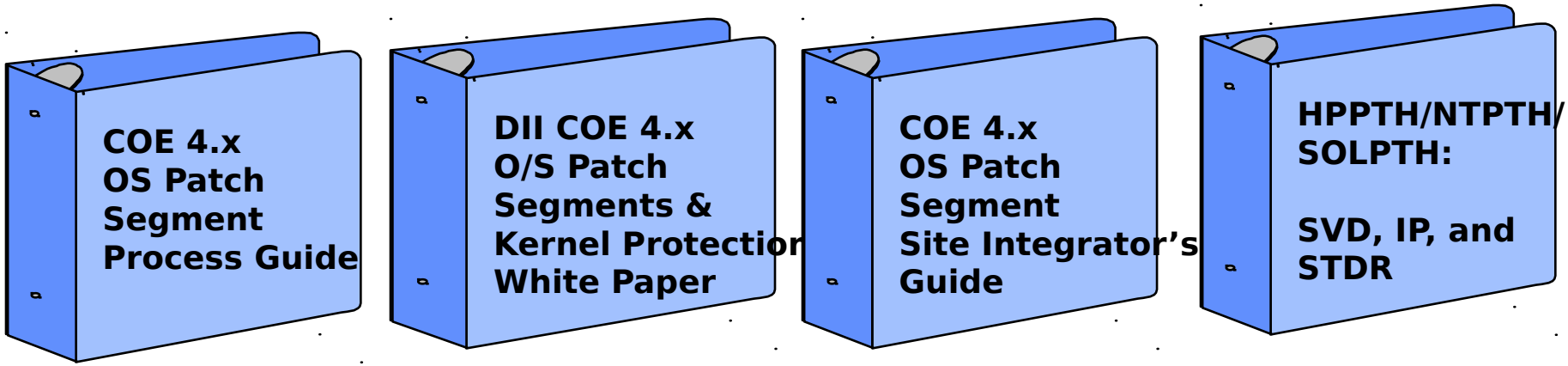
Official COE O/S Patch Segments:					
Prefix	**Version #**	**Operating System**	**COE Baseline**	**CFI Delivery**	**Features**
SOLPTH	3.0.0.8	Solaris 2.5.1	COE 3.x	Dec-99	
SOLPTH	4.1.0.0	Solaris 7	COE 4.x	Feb-00	kernel prot. (4.1.2.0 geared)
HPPTH	4.1.0.0	HP-UX 10.20	COE 3.x & 4.x	Mar-00	kernel prot. (4.1.2.0 geared)
HPPTH	4.1.0.1	HP-UX 10.20	COE 3.x & 4.x	Apr-00	HPPTH 4.1.0.0 minus 'tar' patch
NTPTH	3.0.1.0/SP4-128bit	Windows NT 4.0	COE 3.x & 4.x	Dec-99	SP4 + Y2k & other hotfixes
NTPTH	3.0.2.0/SP4-40bit	Windows NT 4.0	COE 3.x & 4.x	Dec-99	SP4 + Y2k & other hotfixes
NTPTH	4.1.1.0/SP6a-128bit	Windows NT 4.0	COE 3.x & 4.x	Feb-00	SP6a+, kernel prot.
NTPTH	4.1.2.0/SP6a-40bit	Windows NT 4.0	COE 3.x & 4.x	Feb-00	SP6a+, kernel prot
Related O/S Patch Support Segments:					
Prefix	**Version #**	**Operating System**	**COE Baseline**	**CFI Delivery**	**Features**
MSSCE	4.1.2.1	Windows NT 4.0	COE 4.x	Apr-00	incl. MS MMC, SCE
MSSCET	4.1.2.0	Windows NT 4.0	COE 4.x	Dec-99	contains NT lockdown templates

Guidance to OS patch integrators

- ***Site Integrators & developers who plan to create & distribute OS patch segments to their COE community should:***
  - **Obtain/read/absorb any & all available COE & vendor documentation regarding OS patches**
  - **Consider implementing a similar methodology to control process within major COE OS patch segment releases**
  - **Utilize the "template" segment contained within SOLPTH & HPPTH**
  - **After conducting analysis, utilize the backup & restore scripts contained within the COE provided OS patch segments**

Resources for Site Integrators

- ***Resources to aid integrator's & developer's who plan to "roll their own" OS patch segments:***



- **Internet / WWW:**
  - ***http://sunsolve.sun.com***
  - ***http://us-support.external.hp.com***
  - ***http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/allSP6.asp***